26 October 1981

MEMORANDUM FOR: Members, Continuity and Contingency
Working Group

25X1 FROM: [redacted]
Chairman

SUBJECT: Working Group Information

1. Background

As you are aware, the Office of the IHSA has requested your participation in a 2-3 week effort to help them identify the direction the Agency should follow relative to the availability and reliability of IH systems that will be supported in the '85-'89 time frame.

The IHSA has been directed to develop a strategic plan for the Agency's IH systems by the end of August 1982. To accomplish this task within the given time constraints, they have devised a four phase approach. In the first phase (our phase) a series of user oriented working groups will discuss and clarify the goals or objectives of IH from their perspective. The second phase will require other working groups, consisting primarily of IH providers, to address how the goals identified in Phase one might be implemented given technical, space, budgetary and other resource realities. Phase three and four concern themselves with preparing the draft and final versions of the Plan. A schedule for development of the Plan is attached for your information.

2. IHSA Point Papers

The IHSA has prepared two discussion papers that we can use as "strawmen" to focus our views and structure our product. In addition to background information provided, there are a number of specific questions found in both the overview and robustness point papers which will require our response. Since our time is very limited, please give as much thought to these questions and goals as you can prior to our initial gathering

25X1

[redacted]

on the 2nd and 3rd of November. If you can address the quantitative questions early on, so much the better. If you are disposed to committing some of your thoughts to paper for group consideration, please do so.

3. Some Guidelines

a. The time frame for goal implementation is 1985 through 1989. It is assumed that any resources to significantly alter the current plans for IH enhancements would not be available until the FY-85 budget.

b. Our focus should be on requirements and needs, not solutions or implementations.

c. The basic theme of our discussion is simply: What is the magnitude of the dependence that Agency users will place on IH services in the late 80's? Stated differently--At what point does the unavailability of an IH service seriously impact an intelligence function?

d. Recommending changes to the functional capabilities of existing systems is not our concern.

e. We should avoid 'general goodness' suggestions such as commonality and interoperability. These are givens in any IH architectural plan.

f. In addition to the questions and goals posed in the attached point papers, I would welcome any additional topics that you or your components would like addressed.

4. Briefings

We have arranged for a number of tutorial briefings during the first two days to hopefully bring everyone up to speed on the current status, problems and any planned improvements in the availability of the major IH systems. Topics and speakers are listed in the attached schedule. If there are other subjects that you feel would be beneficial to present to the group, please advise [redacted] or myself. 25X1

5. Reference Material

As you can ascertain from the listing attached, there are a number of existing documents which have some relevance to the issue of continuity and contingency. The overview point paper briefly summarizes what we have been able to assemble from these sources. Copies of any of the reference documents may be acquired by calling [redacted] Copies will also be available during the working group deliberations. 25X1

6. I look forward to an informative and productive association. If you have any questions prior to the 2nd, please call [redacted] 25X1

[redacted] 25X1

Attachments:
As Stated

25X1

Next 1 Page(s) In Document Exempt

REFERENCES

Copies of the following publications are available from the Chairman or IHSA representative.

1. OC - Information Handling Survivability Study, dated 3 September 1980

2. ODP - MFR on Emergency Planning, by [redacted] dated 28 October 1980 25X1

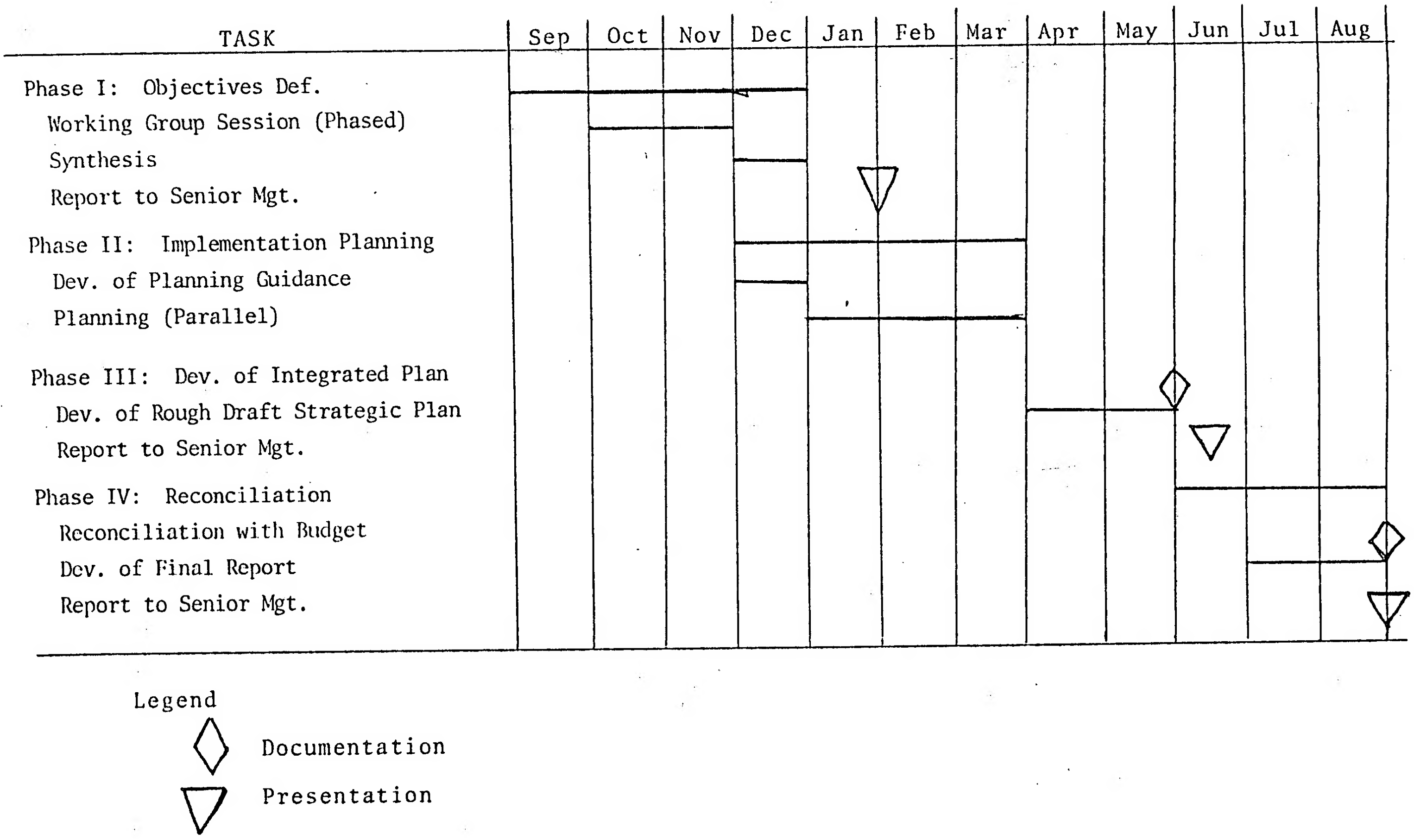
3. NBS - Federal Information Processing Standards (FIPS) Pub 87, Guidelines for ADP Contingency Planning, dated 27 March 1981

4. Processing System Availability Charts covering recent Fiscal Years

5. Communications Planning Issue (Recapitalization Paper), First Two Sections: Challenge and Staff Network, dated 17 August 1981

6. Information Handling Study-1980, Final Report of the Information Handling Task Force, dated 5 September 1980

PLAN FOR IHSs STRATEGIC PLAN



CONFIDENTIAL

Continuity and Contingency Overview Paper

OUTLINE

1. Introduction

   a. Objective
   b. Definitions

2. Current Trends

   a. Political Considerations
   b. Recognition of Need
   c. Architectural Considerations

3. Current Planning Efforts

   a. NIEPS
   b. OC Initiatives
   c. ODP Initiatives
   d. OL Initiatives

4. Threat Assessments

5. Issues

   a. Affordability
   b. Interoperability
   c. Reserve Capacity

6. Discussion Questions

OVERVIEW PAPER

Continuity and Contingency

1. Introduction

a. Objective

The objective of this point paper is to focus attention on system continuity and contingency planning for Agency IHS services. Our intent is to examine the more vulnerable aspects of the Agency's information handling systems (IHSs) identifying critical functions and susceptible choke points, gain perspective from a users view of the criticality of these individual system weaknesses and generate user-backed input for the Agency's IHS Strategic Plan. (For this effort, the scope of threats to be considered exclude the nuclear war concerns of the National Intelligence Emergency Planning Staff (NIEPS) and related activities.)

b. Definitions

Continuity is defined as the capability to sustain the intelligence process when the system is impacted by forces that cause a stressful condition. Contingency planning is those steps that are taken to secure continuity of operations under the circumstances mentioned above. Other terms which describe a system's ability to sustain failure or damage and continue to provide the services that users need include availability, serviceability, reliability and survivability. From a systems view, the term robustness describes these characteristics. It refers to the resilience and reliability of a system -- its ability to continue to function without failure, or given failure or damage, with minimum degradation of performance. In addition, robustness refers to the strength of the system in the sense of its ability to absorb any additional demands that may be placed upon it in a stressed mode.

2. Current Trends

a. Political Unrest

Events of recent past as well as press and intelligence reports have confirmed that the terrorist threat is ever-present and increasing in intensity and sophistication. The vulnerable position 25X1 of [redacted] to terrorist attack has been readily apparent for many years. For example, the Office of Communications has long been concerned about the "all the eggs in one 25X1 basket" problem [redacted] As far back as ten years ago, studies were made addressing [redacted] susceptibility to 25X1 terrorist attack, as well as natural forces and catastrophic failures that might occur within the systems installed there. Over the past decade this situation has only worsened, especially when considered in the light of the many concentrated nodes in the ODP data processing system and the critical choke points that are found within the OC data links throughout the region. (Consult OC Survivability Study.)

When considering contingency plans, the focus of the Office of Communications has traditionally been directed toward the facilities of the foreign network, since that was where the major threat was perceived to be. Today, however, this situation has changed dramatically. In certain cases our facilities may be even less "safe" 25X1 [redacted] Moreover, an evident, heavy concentration of information handling equipment in any one location is almost an open invitation to hostile acts against it. There are, as well, throughout our system a number of fairly evident (and highly critical) architectural choke points. The loss of any one of which may be stifling to maintenance of the intelligence process. There is now much evidence of increased managerial concern for protecting the Agency's IHSs from such a loss. Additional security measures represent only the first tier in providing this protection-- interoperability, expanded capacity, availability, survivability all represent additional and, ultimately, necessary layers in the plan.

b. Recognition of Need

The Intelligence Capabilities for the 1985 Study on Surge Collection and Analysis further confirms the need for an unspecified measure of reserve IH capacity, both fixed and transportable, as well as a robust information handling infrastructure with increased capability to absorb unanticipated sytem demands. Although the Surge paper does not specify, in definitive terms, the extent of the data communications and processing capacity required, the need for an expanded capability in this arena is clearly evidenced.

Also, the EXCOM Staff Long-Range Planning Project of December 1980, CIA Managment Directions for the 1980 CIA Management Directions for the 1980's, affirmed the requirement for flexible and prompt reaction to challenges in the IHS arena. It highlights the destructive impact of constrained fundings in past communications budgets, and the unacceptable risks incurred unless we make the large front-end investments required for a more capable and robust IHS architecture.

c. Architectural Considerations

At the IH systems level a measure of redundancy is usually built in to the design so many internal system failures are covered. The infrastructure which supports the system, however, is often not as well backed-up and, therefore, is subject to single point failures. This is not to argue that our system architecture must be redesigned, for this is neither practical from a physical nor a technical viewpoint. It is to suggest, however, that the largely vertical IHS architecture (see Headquarters Signal Flow Diagram in Robustness point paper as an example) should be critically examined and future systems redesigned accordingly. Current technological developments such as packet technology, will greatly assist in this evolution. In the system robustness paper which follows, this generic problem is explored to greater length and appropriate suggestions are put forward.

3. Current Planning Efforts

a. National Intelligence Emergency Planning (NIEPS)

At the Community level, the NIEPS staff is planning for the information, communications, and personnel requirements needed to support the President and his successors in a national emergency. This effort is focused on continuity of government in the context of strategic nuclear war, as mandated by Presidential Directives (PD/NSC's) 53 and 58.

Within the Agency, the Planning Staff, Office of Plans and Policy, has been assigned responsibility for continuity of operations of the Agency, also primarily in the context of nuclear war. This planning encompasses all types of eventualities, however, and is focused on continuity of the Agency's general foreign intelligence functions. The role of this segment of the DCI's staff is to guide, stimulate, and coordinate the emergency planning of the individual offices within the Agency. Ultimately, the product will be a contingency plan for continuity of vital Agency functions in the event of a catastrophic confrontation. It will be the role of the Planning Staff to coordinate the various initiatives and, to that end, the results of this working group will also be made available. The objective is to bring about an orchestrated, serious and concerted examination of all Agency contingency capability and planning.

b. OC Initiatives

The Information Handling survivability study of 3 September 1980 is the most recent assessment of the survivability of the OC Information handling systems. After a close examination of the communications network, several detailed suggestions are brought forward in this report. Principal among these are the following:

1) Provide high speed data handling capabilities to the foreign field.

2) Improve the connectivity of the Agency's microwave system and explore redundancy in the routing of commercial carrier circuitry.

3) Provide a backhaul capability for the SKYLINK system.

4) Improve the circuitry (and equipment) at the Headquarters building to expand its gateway function in the event of a catastrophic failure [redacted]

25X1

5) Establish a network architecture plan that incorporates the compatiblity requirements of different networks.

If desired, this document is available to participants for further, more detailed examination.

c. ODP Initiatives

The Office of Data Processing has taken several initiatives to also examine its system, identify the vulnerable aspects of it, and recommend approaches to increase the overall system robustness of the Agency's data processing assets. The most recent of these, a 28 October 1980 MFR, is also available to the Working Group for review. The MFR summary highlights several potential problem areas including the need for review of SAFE compatability "not only from the backup concept but also from the manpower, training and user point of view." The MFR, however, is largely directed toward reporting things as they are or have been, and not as ODP would like them to be. It concludes that "plans to develop a capability outside present quarters should wait for a statement of overall Agency policy and guidance." This current exercise is directed toward that end.

d. OL Initiatives

The Headquarters Engineering Branch of the Real Estate and Construction Division, OL is completing a two-month study of alternative actions to improve the reliability/availability of the conditioned power systems. This study looks at some alternative investments and their likely reliability/availability payoffs. The principal consideration and perhaps some of the results from this study will be available to this Working Group as it meets.

4. Threat Assessment

In examining the continuity and contingency question it is useful to first identify the threats that might be expected and, in some fashion, assess their relative likelihood of occurence. The following table presents a categorized listing of such threats. The table represents general hazard groupings which are intended to facilitate easier treatment of the threats that are likely to confront us throughout the ensuing decade. For example, the likelihood of a suborned Agency or contractor employee attempting to sabotage a node or nodes of our IHSs will probably be significant if we find ourselves militarily opposing a Soviet push and we have the same IHS architecture as today. Also, system supportability issues may become more critical as systems become more complex. As used in the Outage

Causes table, maintainability covers the range of conditions that may exist if an IHS product line became materially or technically unsupportable for lack of spare parts, tech training, vendor support, obsolescence, etc.

Participants are requested to complete the table by evaluating the "likelihood of occurence" during the decade of the 80's of each of the 17 specific threats listed. This information along with the "extent of damages expected" should be recorded in their respective columns in terms of very low, low, medium, high and very high. The concern is that we have an architecture that is balanced with respect to risk. That is, a high probability of occurence should correlate with a low level of damage, and a low probability of occurence with a high damage. A threat that provided, for example, a medium probability of occurence and a high damage would represent an elevated level of risk. Such a threat would then be identified as a particular concern.

5. Issues

(1) Affordability

Probably the biggest single issue with respect to continuity and contingency is the priority that should be assigned to these concerns relative to the other concerns (as represented in the other four working groups). Accordingly, at the close of this series of Working Group meetings each participant will be provided a form on which they will be requested to quantify the relative importance of improvements in the IHS concern. Within the scope of this Working Group, however, the assessment of priorities should be qualitative. The dominent concern is ultimately the affordability of continuity and contingency investments.

(2) Interoperability

There, of course, are other valid concepts and concerns such as system interoperability and alternate path processing which may impact heavily on contingency planning. Articulation of critical IHS requirements will assist in identifying candidate systems for enhanced interoperability design. An awareness of opportunities to use interface and protocol specifications, in both planned and current systems design, that will fully exploit IHS interoperability will greatly assist in overall large-scale contingency planning

Probably the best historical example of near-continuous contingency planning within the Agency can be found in the altroute management in the Office of Communications HF network. Before the coming of the satellite era, all overseas field station links were either solely or secondarily HF-dependent and, therefore, assigned to one of several HF Base Stations. However, the very nature of the HF transmission medium as well as the political vulnerability of the individual overseas Base Stations made exercising various failure scenarios within the network a regular monthly necessity.

understood by the participants; over the ensuing decades the procedure became near institutionalized. Although these exercises were, and are, admittedly carried out in a much more restrictive and compatible domain, a similar pattern of back-up operations could well be tailored to strengthen the overall IHS contingency posture.

(3) Reserve Capacity

The Surge Collection and Analysis paper of EXCOM's Intelligence Capabilities, 1985 Study delineates a requirement for rapidly deployable field capabilities and rapidly expandable Headquarters processing capabilities. A major part of providing the surge capability that is desired for the mid-80's is to build enough reserve capacity into the IHS infrastructure to handle unforeseen requirements as they occur. Another major part of surge planning is to have the field-deployable, transportable assets available to bring them to bear on the collection targets when they are needed. By judicious and prudent management of assets that are directed toward continuity and contingency planning it should be possible to also cover much of the surge IHS requirements. The linkages between surge capacity and contingency planning are strong and the capabilities required for one compliments both requirements.

6. Discussion Questions

From experience and the information presented the Working Group is requested to comment on the following questions. Responses should not be limited to a simple endorsement or rejection of the proposition, but should include justifying comments along with any pertinent suggestions they may wish to contribute. All participants are encouraged to voice free and candid opinions in any discussion area.

1. What type of threats are most likely to stress IHS assets during the 1980's? Please fill in the two Outage Table columns. Add explanatory comments as required.

2. What are currently the most critical IHS service failures? What do users want improved first? From a user perspective, are the system availability figures cited in the robustness paper "believable"? How much effect does outbuilding location have on system availability?

3. Should a formal IH system availability improvement program be established? Is it a desirable objective for the IHSA to pursue? As an initial stage of this effort is it feasible to institute a data-gathering exercise for all IHS's (and associated support systems and networks) sufficient to enable sound availability figures to be specified

for each element of the system as well as overall system availability? Given the complexities mentioned, is it reasonable to expect suppliers to collect MTBF and MTTR data on all their IHS-related systems? Should this be a required exercise to justify and schedule system replacement? Should a time phased plan be developed that specifies annual availability improvement figures and ultimate system availability goals for specific systems and baseline conditions?

4. What are the most likely (or anticipated) areas for IHS expenditures in the 1980's? What is likely to be given up in favor of what? What are the options and tradeoffs? How extensively Should IHS expenditures be directed toward contingency capabilities? From a study of the point papers, supplemental information and their own experience, users are asked to make general comments regarding the extent to which they believe IHS resources should be committed to improving the serviceability and survivability of the IHS architecture.

5. Should Agency contingency planning be expanded to include provision for Surge requirements anticipated in the mid 1980's? If so, should this Surge planning include:

   a. Building sufficient and extensive reserve capability into the future IHS architecture to absorb Surge requirements without putting strain (or having negative impact) upon the IH Services that are regularly and routinely provided to the Agency? (It should be recognized that under Surge conditions it is likely that the regular intelligence processes will also be in a highly active mode.)

   b. Providing field-deployable IH systems sufficient to support Surge field requirements for communications, collection and other on-site requirements? (It is anticipated that these systems would normally be transportable and have a high degree of mobility and versatility built into the various deployment schemes.)

IHS Outage Causes Table

	Likelihood of Threat Occurence During 1980's	Extent of Damages to IHS Capability If Threat Occurs
A. System Forced		
1. Internal System Failures		
a. Spontaneous Component Failure		
b. Operator Error		
c. System Maintainability (NORS, NORM)		
2. Agency Support Failures		
a. Power Generator or UPS		
b. Air Conditioning or Water Supply		
c. Communication Lines/Links		
B. Outside-Agent Forced		
1. Natural Causes		
a. Extreme Weather		
b. Flood		
c. Fire		
d. Untenability		
2. Accidental Causes		
a. External Utility Failures		
b. Fire		
c. Water		
d. Operator Accident		
3. Aggression Caused		
a. Deliberate System Tampering		
b. Sabotage		
c. Terrorist Attack		
d. Armed Conflict		

Robustness

I. Background

The constrained budget environment of the past six or eight years and the government-wide zero based budgeting process have taken their toll on the Agency Information Handling Systems (IHS). We now have an environment that is near an optimum with respect to cost versus performance. Concomitantly, our systems are fragile. For the most part, it is a single thread environment. As a broad generalization, there are a large number of single points of failure in our IHSs; it is far too likely that any single failure will bring down a system, albeit perhaps, only briefly.

This lack of robustness of our systems will not be acceptable for our foreseeable future. The Agency has an ever increasing level of on-line, real-time operational responsibilities. Furthermore, it must provide continuity of operation during contingencies and war. The current robustness of our IHSs falls far short of serving these needs. It provides inadequate availability for the projected numbers of users of communications and data processing functionalities for the mid-80's, and inadequate survivability in the advent that hostile action or an accident disables a major functional entity.

The reason that the current situation exists, of course, is that robustness costs money and contributes little, if anything, to performance. To improve robustness, we have to invest in it, perhaps at the expense of providing other IHS functionalities. (Such a tradeoff will always obtain, because there will always be more things on our "wish" list than there are funds to implement them.) As a consequence, we have to be careful in specifying robustness objectives. It is tempting to specify lofty goals, but it should be recognized that accomplishment of these goals costs, in terms of other things not done. The problem is intensified because the cost of availability tends to rise exponentially as the level approaches 1.0.

Since there will be acute limitations of funds in the light of all the objectives the Agency has for new IHS functionalities, the governing philosophy should probably be for the Agency to work its way out of the fragility corner via the planned evolution of the architecture. As we develop new capabilities we should assure that they meet our robustness criteria and provide architectural redundancy with respect to current systems. We should not modify the existing systems simply to improve robustness--that is simply unaffordable.

While the robustness objectives of the IHS strategic plan need to be specific to be meaningful, it should be recognized that they are not based on hard analyses. These will have to come later, and they will doubtless result in some modification of our goals. But by being specific at this point, it is possible to assure a common understanding and mutual agreement as to what we need to accomplish, relative to where we are today.

II. Status

1. Measurement of System Availability

The issue of availability is made more complex by the fact that there are some definitional problems relevant to the terms "availability." For hardware, intrinsic availability, A_O, is defined as:

$$A_O = \frac{MTBF}{MTBF + MTTR}$$

MTBF - Mean time between failures

MTTR - Mean time to repair

That is the definition we currently use, but it is recognized that it has significant shortcomings in the IHS environment. Principally, these shortcomings are:

- A momentary "spike," or system outage is not uncommon and can have major impact in the IHS environment. Although such a spike can destroy a considerable amount of in-process processing and contaminate electronic files, the effect on the numerical values of availability is negligible.

- An on-line system can slow down quite sharply when its task load approaches system saturation. Technically, the system has not failed, yet its performance may be clearly unsatisfactory.

- There may be occasional, complex software errors in such elements as the operation system, transaction handler, or communications elements of the systems software. These errors are frequently so difficult to diagnose that recourse is had to temporary "work arounds," which deflect the flow of the processing either back to the user or into some non-ideal channel. Such deflections are equivalent to either a loss of time or a degraded operational mode, yet do not count as an availability reduction.

Numerous proposals for new definitions of availability for the IHS environment have been made in the professional literature. To date, there is not a consensus with regard to any of these, and thus a clear and reasonably complete specification of IHS availability is not available. For the purpose of this planning effort, it is recommended that we proceed with the current hardware systems availability definition presented above.

2. Central DP Services

When the SAFE system comes on-line in 1983, there will be three central systems in the Headquarters area: the Ruffing Computer Center (RCC), the Special Computer Center (SCC), and SAFE. In addition, there are numerous other systems dedicated to specific operational functions, and some standalone general purpose mini-computers.

The RCC has grown in numbers of computers over a period of years, reaching its current status of seven large, general purpose computers in June 1978. Principally, needed capacity growth from this point on has been achieved by replacing existing processors with newer technology ones of greater power. The installation currently has three IBM 370/168's, an IBM 370/158, an IBM 3033MP, an IBM 3033 UP, and an Amdahl V-8, all served by three COMTENs. Several hundred disk drives and tape devices provide bulk memory for the RCC. The Center provides three types of services: VM, GIMS, and batch. In general, each of the mainframes is dedicated to one of these services.

The SCC consists of four mainframes: two Amdahl V-6's and two IBM 370/158's. CAMS currently runs on one of the Amdahl's, but CAMS II development will be done on a 168 at a remote site in the Washington area.

Currently the backup computer capability that we have is pretty much limited to intracenter transfers of workload. We have not had to test intercenter backup, but there is hardware compatability and a communications link between the RCC and SCC which should permit it, should the need arise.

The proportion of IHSs dedicated to on-line functions has grown steadily. Historical data for the RCC indicates an exponentially growing level of simultaneous on-line users, averaging 20 percent per year. Data available on user expectations for utilization in the near term future indicates that an extrapolation of this historical data could produce a projection that would be low. All indications are that central system utilization over the next several years will be at a substantially higher percentage growth rate that is limited by communications and central processing capabilities, rather than being demand determined.

Based on the A_O availability definition in the previous section, ODP reports a Ruffing Computer Center system intrinsic availability of about 0.97. User perception is usually that it is not as good as this, however, and the difference clearly lies in the sort of definitional shortcomings described in association with the definition.

Figures 1, 2, and 3 provide representative data from ODP's most recent computer system quarterly report. From these figures it is possible to get a feel for the operating environment we have today. Additionally, table 1 presents the availability and MTBF for each of the major services at the quarterly reporting points.

The value of 0.97 is certainly comparable with the best values obtaining commercially today. It is a satisfactory level when supporting the approximately [redacted] simultaneous, on-line users that we do today. It is, in fact, a remarkable value when it is recognized that the centers are comprised of components for which the contractually committeed availability is 0.90. However, maybe in five years, the number of simultaneous on-line users could be an order of magnitude greater. At such a level, 0.97 is no longer acceptable; availability must be significantly better.

25X1

If we maintain the lost work due to system failure at the same level as today, a ten-fold increase in simultaneous on-line users would correlate with an availability of 0.997. If we specify no more than one lost hour in a work month of 9 hours days, we are talking about A_o = 0.995. Also, the SAFE system has specified an availability of 0.997. The fact that these approaches produce such similar values argues that our availability objective should be in this range.

The increase from A_o = 0.97 to approximately 0.997 for ODP's central systems has major IHS system implications. It means we must have:

- o better component reliability
- o greater redundancy in the context of greater system flexibility
- o system architecture with reduced single points of failure
- o system architecture with improved fail soft character
- o superior design for maintainability

The requirement for greater reliability is going to have an impact on the way we procure equipment. GSA schedule EDP equipment has an individually negotiated availability of 0.90, based on roughly comparable duty requirements. There has been a traditional reluctance in the computer industry to bid on RAM-type (Reliability, Availability and Maintainability) performance characteristics for equipment. Most

25X1

Next 3 Page(s) In Document Exempt

component suppliers have been demurring at the suggestion of bidding to higher levels of availability in non-schedule procurements. That reluctance has recently been decreasing, however, as a high reliability market emerges. A few suppliers such as Hewlett-Packard, Tandem, and Wang, now specifically market their higher equipment reliabilities - values of 0.98 or greater.

To achieve a 0.997 system availability without unacceptable redundancy and component sparing, individual components should provide even better reliability. The implication is that we need to develop an approach to procuring a very high level of IHS components' reliability in a competitive environment.

3. Communications System Availability

To maintain the required level of services the Office of Communications has traditionally designed the communications switches with a high degree of built-in system redundancy. The pay-off has, of course, been reflected in terms of very good individual system availability figures. (See Table 2 for FY-1981 figures.) System availability has been maintained at a high level for quite some time despite the continued aging and questionable supportability of the MAX switches.

These figures do not, however, reflect overall end-to-end system availability. To determine this quantity for a particular service location, the overall ability of the transmission link and terminal equipment must also be included in the composite availability figure. (Individual terminal equipment availability probably would not have much impact, however, since very high availability is usually achieved by immediate "sparing off" to reserve equipment.)

Table 2

	System	Availability (A)
	MAX (avg of 3)	99.92
25X1	MAX-1A [redacted]	99.994
	MAX-II [redacted]	99.894
	MAX-III [redacted]	99.882
	ARS (avg of 4)	99.52
25X1	ARS [redacted]	99.779
	ARS [redacted]	99.533
	*ARS [redacted]	99.624
	ARS [redacted]	99.114
	CDS (A_O)	99.5
	DATEX (A_O)	99.0
	ACT-0 (A_O)	99.5

* System was deactivated circa 1 April 1981.

Table 3 is a compilation of the overseas communications system outage figure for both the computer switches and the overseas transmission media. This table provides instances of outage from whatever source in these two generic domains. Traditionally, the quality of the communications link is measured in number of hours of carrier outage per month, and is so logged for reporting by overseas communications operators.

Availability values for various services, such as provided by ODP, are more difficult to measure in the case of communications data links because of the great intricacy of the various networks and the time-variable scheduling of service to the overseas stations. This intricacy is illustrated in figure 4, showing just the major electronic traffic paths within the Headquarters building.

To develop an accurate system availability, A_o , figure for any particular data service link the end-to-end system availability has to be taken into account. When the effect of time-variable scheduling of service resources coupled with the many combinations of transmission systems external to the building is considered, the complexity of accurately presenting A_o on a representative circuit is escalated considerably. End-to-end circuit availability figures have not, therefore, been routinely provided to the user community, although an effort is currently underway to do this for the data transmission links in the foreign network. Better documentation was a recommendation of the 1980 OC Survivability Study.

In general, however, overall communication system availability is perceived to be comparable to that of the data processing systems. Consider a cable flow to the DDO from [redacted] This traffic is processed through the following systems: ARS [redacted] ARS (Hqs), MAX-III, MAX-II, and CDS. Neglecting the effect of carrier and station service hardware, these devices provide a circuit availability of 0.982. This is actually an upper limit, since the effect of the overall transmission media will degrade it slightly. 25X1 25X1

An area that has been a recognized availability problem is the data links to the Headquarters area outbuildings. This is most noticeably reflected in the availability seen by ODP terminals users in these buildings. Although no data is regularly collected on the availability of these links, it is generally perceived by users to fall well below that of ODP's central systems, which the terminals' users are accessing.

25X1 [redacted]

25X1

Next 2 Page(s) In Document Exempt

[redacted] 25X1

5. Utilities

An additional dimension of the robustness concern is the provision of support services, primarily power and cooling water. Emergency power for Headquarters is provided by a three-sector system: five diesel powered emergency generators, five uninterrupted power systems (UPSs), and a complex, relay-based system to control the emergency power start-up and system insertion. Elsewhere, such as [redacted] 25X1
25X1 the configuration is basically the same, although smaller and simpler.

Most of the UPS failures--that is failures to provide uninterrupted power when the VEPCO power falters or fails--have been traced to electrical and mechanical stress in the control systems. The UPS control systems currently employed involve a hybrid of solid state and relay technologies. Some of this technology is now fairly dated, reflecting the age of the equipment. The control logic for the three sectors of the Headquarters area systems is implemented primarily in terms of relays. It is a large -scale system and such relay control systems are tricky in terms of logic. It is difficult to test such systems for all possible event sequences, so they frequently have unproven sequences. Like any relay system, they may also have intermittent failures in proven sequences. The latter most frequently occur as a consequence of electrical stress affecting relay actions in a way which modifes the intended logic. (Modification of required make -before-break or break-before-make sequencing is a frequent logic corruption, unique to relay systems, which can be produced by electrical stress.)

A significant portion of the current data processing system failures are caused by support systems. Providing system availabilities of the level specified for SAFE, 0.997, is not possible without upgrading the reliability of these systems. Such investments should be considered in two areas: reliability and capacity. The principal reliability concern is the control systems. Some of these,
25X1 as in the case of [redacted] UPS, are intrinsic to vendor supplied equipment. Headquarters has an Agency -developed, relay-based control system containing approximately 2000 relays. Capacity improvements are required if terminal local nets, local nets, with their associated disk files, and mini-computers are to be protected by UPSs, in the same manner as are the central facilities.

As a reference point, the approximate cost of providing UPS power throughout the new headquarters compound building is estimated at $5 million. This produces an allocated cost of $1667 for each of the

25X1 [redacted] To retrofit the existing building to provide the same total coverage might cost 50 percent more per person. Our recent VEPCO experience is that there are about 20 spikes or short term voltage drops which exceed equipment tolerances per year and one to three outages.

6. System Architecture: Current and Required

Today we do not have an Agency IHS architecture; we have a group of architectures. There are the central processing systems, the overseas communications system, the SAFE system and the NPIC Data System, to name a few. As the loads on these systems increase, coupled with user demands for interoperational capabilities, the importance of an overall architecture rapidly increases.

Certainly one of the most important current concerns with respect to architectural definition is robustness. The architecture has to be designed in the light of the system risks. The principal ones are:

- o Failure of a key component - usually one at a single point of failure
- o System design or implementation shortcoming that results in information spillage
- o Substantial damage by accident or natural causes
- o Sabotage by an Agency employee or facility-cleared contractor
- o Terrorist acts
- o Conventional war
- o Strategic war

The emphasis we have placed on these risks in the design of our systems is approximately in the order in which they are listed. That none has had strong relationship to funding is seen in the fact that there are over 30 single points of failure in the RCC system. That is not the way anybody would like to have it; it is the product of cost performance optimization in a severely strained budget environment. The other risks have been accorded progressively less concern, and the last three, hardly any. Those that rely heavily, or totally, on a single functional node, such as NFAC on the RCC, are in an extremely vulnerable position with respect to the last five risks.

25X1 [redacted]

25X1

SECRET

[redacted]

A remote backup facility would provide a much more robust environment with respect to the data processing and communications functions than we now have. To meet operational objectives and be cost effective, it should probably meet the following criteria:

- o Support combined data processing and communications functions.

- o Have a "critical mass" that would permit it to maintain an adequate level of IHS functions to meet Agency operational responsibilities, given

25X1 [redacted]

- o Be located at least 100 miles outside the Washington metropolitan area. (A location well south of Washington would permit a higher, and thus less vulnerable satellite antenna attitude.)

- o Have some colocated Agency operational function that require extensive use of the data processing and communications facilities. (Only such normal daily loading of the facility would assure its continuous operational values to support emergency operations.)

25X1 [redacted]

SECRET

25X1 [redacted]

The cost of a remote backup facility may not be as substantial as it would first appear. The data procaessing equipment could be almost totally provided from existing stock and much of the communication equipment may be similarly available as well. (ODP creates excess mainframes when it has to buy larger, new technology machines to meet demand. OC will have switching facilities - principally the Network Switching Centers (NSC's) - that MERCURY will provide, which perhaps could be placed in a remote site instead of Headquarters. On this basis, the investment required in a remote facility is principally in the facility itself, cryptographic and communications link equipment, and any extra cost associated with concealment and deception relevant to the function of the facility.

Whether such a remote facility alternatively makes sense depends on two key factors in addition to IHS fragility overseas: the level of the threat and cost. An expert assessment of the threat is beyond the purview of this strategic planning activity. Determination of the cost can only come as the product of concentrated study by a small team dedicated to the evaluation of the issue. In fact, any such evaluation should develop alternatives configurations in a gradation of capability, and cost, corresponding to those alternatives.

In summary, the elements of physical security to be considered in response to the various threats to IHSs include:

- Physical separation of primary resources

- Mutual backup of separated facilities to provide system fail-soft operational characteristic

- Provision for a backup facility, of a specified "critical mass," more than a hundred miles away from Headquarters

- Greater physical protection of each resource center to increase the closest point of approach of a sabotage-type threat

- Even more stringent access control to vital resource spaces, e.g., special personnel identification cards with associated monitoring equipment.

There are also electronic architectural concerns. The electronic and physical architectural issues concerning robustness are coupled. The capability for mutual backup of physically separated facilities puts a substantial additional constraint on the electronic architecture. One of the chief elements of this electronics architectural constraint is that the hosted functionalities be performable on an alternative resource of lesser scale, and perhaps simpler architecture. There are, however, electronic architectures for central systems, which essentially preempt backup within the context of practical cost. Local nets suffer from the fact that, lacking dedicated operational personnel, backup discipline will be loosely applied. As a consequence, wherever precious data is involved, it should be stored either on a central system or a mini-computer system large enough to have dedicated operational personnel.

III. Issues

1. How Important is Improved Availability of IHS Services?

This question refers to "routine" failures of components. The answer,of course, varying somewhat with the type of service. The issue is the level of availability that we need to support Agency operational needs.

In the foregoing discussion it was suggested that one rationale for setting A_0 goals is to provide a constant loss of manhours, or investment, with failures. In this context, if MTTR is a constant, then the MTBF required is proportional to such parameters as the number of logged users on VM or the batch CPU time. (Evaluation of MTTR's implied by table 1 indicates remarkable constancy: about 1 hour.) If MTTR can be progressively reduced with increasing MTBF, then the increase in MTBF might not have to be so great. Other rationales might be considered, but there should be some rationale to guide this objective.

The base issue is identified as how important is the availability, rather than what should it be, because the latter is subject to competing priorities and implementation engineering realities. Improved availability is going to require investment, and the question is ultimately going to be, What is it worth?

2. What is the Requirement for Assured IHS Capabilities?

In considering the requirements for mutual backup of headquarters central processing facilities and for a backup facility, the first question is, What is the priority and requirement for assured IHS capabilities? These are capabilities whose availability must be restored within a specified time to avoid significant damage to national intelligence operations.

Since this is a first, crude look at such a question, the answer should not be expected to be precise. The word "significant" is itself not precise. Ultimately, one might like to consider categories of mission importance, but that appears to be beyond the scope of this initial effort. The current objective is to get a sense for the scope of the requirement for assured IHS capabilities, and from this, to infer the requirement for backup capabilities.

In table 2 is presented the consumption of ODP's resources in 1981 by the larger operational systems. In table 3 are the component-funded systems. Hopefully, the systems in these two tables are also most of the important ones with respect to Agency operations. There may be others, however, of lesser size which are of equivalent importance. If so, they should be added. The requirement for assured capabilities should be based on evaluation of the specific systems of the Agency, as presented in tables 2 and 3.

3. How Important is it to Upgrade Contingency Utilities?

Currently, we only have UPS power conditioning for central communications and data processing facilities in the Washington metropolitan area buildings. How important is it to retrofit such
25X1 buildings as headquarters, [redacted] to provide total power conditioning? (It is assumed that our tenancy in the other metropolitan area buildings is sufficiently short-term that their retrofit is clearly not warranted. This assumption should be verified, however.)

A convenient measure in evaluating this issue may be the investment required per person. Is this investment considered worthwhile? With what priority? Since the value of each total conditioning strongly relates to the installation of terminals and local nets, the time phasing of such total power conditioning should relate to the terminal installation goals developed by the Information Handling Facilities working group.

The reliability of the existing UPS systems which support the central system is also a legitimate dimension of this issue. Since this is an integral aspect of the availability of the central systems, it is probably best dealt with in this context, however.

IV. Discussion Questions

The following are a list of questions which probably need to be answered in order to deal successfully with the foregoing issues.

1. What IHS functions are most critical to Agency users? How long can the unavailability of each of the systems listed in tables 4 and 5 be sustained before there is significant damage to operational intelligence functions? Please complete tables 4 and 5 by selecting time groupings for each system and also indicate your estimate of desired A_o . For like systems, what are the best estimates of system availability figures that users will require in the 1985 to 1989 timeframe? On this basis, what functionalities or systems need to be backed up against a normal host center loss? What does all of this add up to in terms of non-Washington area backup capability?

2. What opportunities have been identified for non-Agency processing in a capacity-loss contingency? Have they been explored with respect to security acceptability and compatibility? Have then been tested in the backup mode?

3. How damaging to Agency operational functions would be the loss [redacted] or a major computer center? Is the risk high enough to warrant an investment in a detailed evaluation of a remote facility? 25X1

4. What priority should be given, in general, to development of contingency capabilities for IHSs? For example, is the investment and disruption associated with development and testing for identified mutual backups worthwhile? Should simulated failure exercises be conducted on a regular basis to validate the back-up capability?

5. What are the availability implications of a local processing capability for identified functionalities? It should be recognized that for such local capabilities:

   - Overall functional availability may well be less unless complete data base and application software compatibility with central systems exists.

   - Backup is likely to be unreliably performed unless dedicated operational personnel are provided.

   (Complete compatibility = software runs either centrally or locally, without modification, and files use the same DBMS in both environments and can be transferred in either direction.)

6. What sort of new approaches might be evaluated in the next phase of this planning effort to obtain high reliability machinery in a competitive procurement environment? For example, can we make audit of supplier quality assurance processes and procedures an element of a proposal evaluation?; Are there instances where we should require that suppliers provide verified reliability data from independent test laboratories in their proposals?; and Should we plan statistically designed acceptance test and evaluation of a sample lot of equipment?

25X1

Next 3 Page(s) In Document Exempt